

## B 5.11 Apache-Webserver

### Beschreibung

Der Apache-Webserver ist seit 1997 der bei weitem am häufigsten eingesetzte Webserver. Laut der Netcraft-Webserverstatistik war im August 2002 auf über 60 Prozent aller betrachteten Webserver ein Apache-Webserver im Einsatz.

Der Apache-Webserver entstand 1995 aus dem bis dahin meist genutzten Webserver, dem *NCSA httpd*, der am National Center for Supercomputing Applications der University of Illinois entwickelt worden war. Da der bisherige Entwickler, Rob McCool, das NCSA verlassen hatte, war die Entwicklung ins Stocken geraten. Eine Gruppe von Webmastern fand sich zusammen, um den *NCSA httpd* weiter zu entwickeln. Da die Weiterentwicklung zunächst in der Form von Patches und Ergänzungen zum *NCSA httpd* erfolgte, bekam das Produkt Namen Apache, von "A patchy server".

Ende 1995 wurde die Version 1.0 des Apache-Webserver veröffentlicht. Nach einer längeren Beta-testphase für die Version 2, die sich seit ungefähr 1998 in der Entwicklung befand, wurde im April 2002 mit der Version 2.0.35 die erste "Produktionsversion", beim Apache-Webserver *General Availability Release* genannt, freigegeben.

In der neuen Version des Apache-Webserver hat sich vor allem an der Architektur des Apache-Kerns einiges geändert. Bei der Entwicklung der neuen Version hatten die Autoren das Ziel, die Portierung auf neue Plattformen einfacher zu gestalten, und entwarfen eine modulare Architektur, in der die *Apache Portable Runtime* (APR) eine Abstraktionsschicht zwischen dem unterliegenden Betriebssystem und dem Apache 2.0 darstellt. Die APR stellt für die eigentlichen Apache-Module gewissermaßen ein virtuelles Betriebssystem dar, verwendet aber so weit wie möglich native Betriebssystemaufrufe, um eine bestmögliche Performance zu erzielen.

### Gefährdungslage

Für den Grundschatz werden pauschal die folgenden Gefährdungen als typisch für einen Apache-Webserver angenommen:

#### Organisatorische Mängel:

- [G 2.1](#) Fehlende oder unzureichende Regelungen
- [G 2.9](#) Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- [G 2.87](#) Verwendung unsicherer Protokolle in öffentlichen Netzen
- [G 2.97](#) Unzureichende Notfallplanung bei einem Apache-Webserver

#### Menschliche Fehlhandlungen:

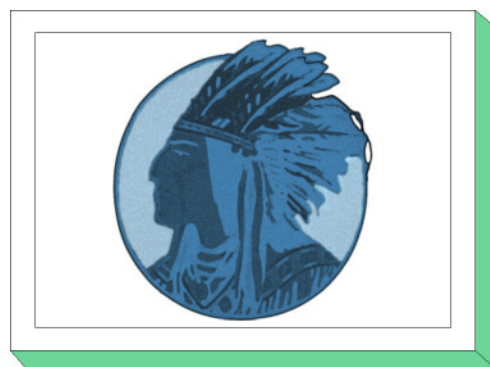
- [G 3.1](#) Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- [G 3.9](#) Fehlerhafte Administration des IT-Systems
- [G 3.38](#) Konfigurations- und Bedienungsfehler
- [G 3.62](#) Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver
- [G 3.63](#) Fehlerhafte Konfiguration eines Apache-Webserver

#### Technisches Versagen:

- [G 4.39](#) Software-Konzeptionsfehler

#### Vorsätzliche Handlungen:

- [G 5.2](#) Manipulation an Daten oder Software



- [G 5.7](#) Abhören von Leitungen
- [G 5.21](#) Trojanische Pferde
- [G 5.28](#) Verhinderung von Diensten
- [G 5.71](#) Vertraulichkeitsverlust schützenswerter Informationen
- [G 5.85](#) Integritätsverlust schützenswerter Informationen
- [G 5.109](#) Ausnutzen systemspezifischer Schwachstellen beim Apache-Webserver

### Maßnahmenempfehlungen

Seit Version 2 wird neben diversen Unix-Varianten auch Windows als Betriebssystemplattform für den Apache-Webserver voll unterstützt. Zwar gab es auch eine Portierung der Version 1.3 auf Windows, diese galt jedoch bis zuletzt als nicht so stabil wie die Unix-Versionen. Die Maßnahmen in diesem Baustein sind so weit wie möglich so formuliert, dass sie sich sowohl auf einen Apache-Webserver unter Unix als auch unter Windows anwenden lassen. An einigen Stellen wird auf betriebs-systemspezifische Aspekte besonders eingegangen.

Für die sichere Planung, Implementierung und den sicheren Betrieb eines Apache-Webservers müssen zunächst die allgemeinen Aspekte berücksichtigt werden, die im Baustein B 5.4 *Webserver* erläutert werden. In diesem Baustein werden vor allem solche Aspekte der Sicherheit betrachtet, die über die allgemeinen Aspekte hinaus speziell für einen Apache-Webserver relevant sind.

Im Rahmen der allgemeinen Planung für den Aufbau eines Webangebots (siehe [M 2.172](#) *Entwicklung eines Konzeptes für die WWW-Nutzung*) wird entschieden, zu welchem Zweck das Webangebot dienen soll und an welche Zielgruppen es sich richtet. Ist im Anschluß daran die Entscheidung gefallen, dass das Webangebot mit einem Apache-Webserver aufgebaut werden soll, muss sich eine detailliertere Planung für dessen Einsatz anschließen (siehe [M 2.269](#) *Planung des Einsatzes eines Apache-Web-servers*). Soll der Apache-Webserver in Verbindung mit SSL eingesetzt werden, so muss dies früh-zeitig in die Planung einbezogen werden (siehe [M 2.270](#) *Planung des SSL-Einsatzes beim Apache-Webserver*). Der Einsatz von SSL erfordert auch beim Betrieb des Servers einige zusätzliche Maß-nahmen (siehe [M 5.107](#) *Verwendung von SSL im Apache-Webserver*).

Die Administratoren müssen für die sichere Installation und den sicheren Betrieb eines Apache-Web-servers geschult werden. Wichtige Aspekte, die in einer solchen Schulung abgedeckt werden sollten, sind in [M 3.37](#) *Schulung der Administratoren eines Apache-Webservers* beschrieben.

Bevor der Apache-Webserver auf dem Serverrechner installiert wird, muss zunächst das Betriebs-system geeignet konfiguriert und abgesichert werden (siehe [M 4.192](#) *Konfiguration des Betriebs-systems für einen Apache-Webserver*). Die Integrität und Authentizität der zur Installation verwendeten Pakete (Quelltext- oder Binärpakete) muss überprüft werden (siehe [M 4.191](#) *Überprüfung der Integrität und Authentizität der Apache-Pakete*). Bei der eigentlichen Installation und der anschließenden Grundkonfiguration sind eine Reihe von Punkten zu beachten, die in [M 4.193](#) *Sichere Installation eines Apache-Webservers* und [M 4.194](#) *Sichere Grundkonfiguration eines Apache-Webservers* be-schrieben werden.

Sollen auf dem Webserver Bereiche nicht öffentlich, sondern nur einem begrenzten Kreis von Be-suchern zugänglich sein, so ist [M 4.195](#) *Konfiguration der Zugriffssteuerung beim Apache-Webserver* zu beachten. Beim Betrieb eines Apache-Webservers sind außerdem die in [M 4.196](#) *Sicherer Betrieb eines Apache-Webservers* beschriebenen Aspekte zu beachten.

Falls auf dem Apache-Webserver dynamische Webseiten über Server-Side-Includes, cgi-Programme oder andere Servererweiterungen realisiert werden sollen, so ist [M 4.197](#) *Servererweiterungen für dynamische Webseiten beim Apache-Webserver* zu berücksichtigen. Der Apache-Webserver kann zur Erhöhung der Systemsicherheit unter verschiedenen Unix-Varianten in einem sogenannten chroot-Käfig installiert werden (siehe [M 4.198](#) *Installation eines Apache-Webservers in einem chroot-Käfig*).

Einige Punkte, die bei der Notfallplanung zusätzlich zu den allgemeinen Aspekten der Notfallplanung speziell für einen Apache-Webserver berücksichtigt werden müssen, sind in [M 6.89](#) *Notfallvorsorge für einen Apache-Webserver* zusammen gefasst.

In Beispielen und bei konkreten Empfehlungen wird im Rahmen dieses Bausteins von Version 2.0 eines Apache-Webserver ausgegangen. Wo nicht explizit auf einen Unterschied hingewiesen wird, sollten jedoch die meisten Aussagen auch für die Version 1.3 gelten. Beispiele werden meist in der Syntax angegeben, wie sie für einen Apache-Webserver unter Unix korrekt ist, sie sind aber ohne große Mühe auf die Windows-Version übertragbar.

Nachfolgend sind die Maßnahmen zur Umsetzung von IT-Grundschutz für den Apache-Webserver zusammengefasst. Die Maßnahmen des allgemeinen Webserver-Bausteins und der anderen relevanten Bausteine werden aus Gründen der Übersichtlichkeit hier nicht noch einmal aufgeführt.

### **Planung und Konzeption**

- [M 2.269](#) (A) Planung des Einsatzes eines Apache-Webserver
- [M 2.270](#) (Z) Planung des SSL-Einsatzes beim Apache Webserver

### **Beschaffung**

- [M 4.191](#) (A) Überprüfung der Integrität und Authentizität der Apache-Pakete

### **Umsetzung**

- [M 3.37](#) (A) Schulung der Administratoren eines Apache-Webserver
- [M 4.192](#) (A) Konfiguration des Betriebssystems für einen Apache-Webserver
- [M 4.193](#) (A) Sichere Installation eines Apache-Webserver
- [M 4.194](#) (A) Sichere Grundkonfiguration eines Apache-Webserver
- [M 4.195](#) (A) Konfiguration der Zugriffssteuerung beim Apache-Webserver
- [M 4.197](#) (B) Servererweiterungen für dynamische Webseiten beim Apache-Webserver
- [M 4.198](#) (Z) Installation eines Apache-Webserver in einem chroot-Käfig
- [M 5.107](#) (Z) Verwendung von SSL im Apache-Webserver

### **Betrieb**

- [M 4.196](#) (B) Sicherer Betrieb eines Apache-Webserver

### **Notfallvorsorge**

- [M 6.89](#) (A) Notfallvorsorge für einen Apache-Webserver